🛡️ Introduction to CyberSecurity

Cybersecurity is broadly categorized into two major areas:

1. Offensive Security
2. Defensive Security

🔒 1. ***Offensive Security***

Offensive security focuses on **breaking into systems**, **exploiting vulnerabilities**, and **finding loopholes** to simulate what an attacker might do. The ultimate goal is to understand hacker techniques and enhance system defenses.

🔍 Key Roles in Offensive Security:

- **Penetration Tester**
  Tests technology products for exploitable security vulnerabilities.

- **Red Teamer**
  Acts as an adversary, attacking an organization to provide feedback from an enemy's perspective.

- **Security Engineer**
  Designs, monitors, and maintains security controls, networks, and systems to prevent cyberattacks.

> Red Teams and Penetration Testers specialize in offensive techniques.

🛡️ 2. ***Defensive Security***

Defensive security focuses on **preventing intrusions** and **detecting/responding** when they occur. Blue teams are responsible for these activities.

🔐 Main Objectives:

- Prevent intrusions
- Detect intrusions
- Respond to incidents appropriately

🧰 Common Defensive Security Tasks:

- **User Cybersecurity Awareness**
  Educating users about phishing, password hygiene, and social engineering.

- **Asset Management**
  Documenting and managing systems/devices to be secured.

- **System Updates & Patching**
  Keeping all systems updated to prevent exploitation of known vulnerabilities.

- **Preventative Security Devices**
  Using firewalls and Intrusion Prevention Systems (IPS) to filter traffic.
- **Logging & Monitoring**
  Detecting unauthorized devices and suspicious behavior through effective monitoring.

🧭 3. ***Areas of Defensive Security***

🟢 Security Operations Center (SOC)

A **SOC** is a team of cybersecurity professionals that monitor systems and networks to detect malicious events.

Key Responsibilities:

- **Vulnerability Management**
  Fixing or mitigating system weaknesses.
- **Policy Violation Monitoring**
  Ensuring users adhere to security policies.
- **Unauthorized Activity Detection**
  Identifying stolen credentials or abnormal access behavior.
- **Intrusion Detection**
  Recognizing attacks like malicious links or server exploits.

🧠 Threat Intelligence

Threat Intelligence is about gathering and analyzing information related to **actual or potential cyber threats**.

Key Concepts:

- Intelligence is gathered from logs, forums, and threat feeds.
- Data is collected, processed, and analyzed to detect adversary patterns.
- Helps predict attacker behavior and supports **threat-informed defense**.

> ***Examples of threat actors:***
>
> - ***Nation-state cyber armies***
> - ***Ransomware gangs***
> - ***Hacktivists***

🛠️ **Open-Source Tools:**

- **AbuseIPDB** – Check IP reputation and report malicious IPs
- **Cisco Talos Intelligence** – Threat detection and investigation

> Security analysts use these tools for alert investigation and reputation checks. You can contribute to a safer internet by reporting bad actors.

🔬 *Digital Forensics and Incident Response (DFIR)*

DFIR involves **investigating cyber incidents**, understanding the attack, and initiating proper responses.

🗂 1. *Digital Forensics*

Focuses on analyzing:

- **File Systems** – Revealing installed, deleted, and hidden files
- **System Memory** – Capturing malware in memory-only operations
- **System Logs** – Identifying anomalies and attack footprints
- **Network Logs** – Understanding attack patterns through traffic analysis

🚨 2. Incident Response

Incident response outlines how to react to data breaches, malware outbreaks, and intrusions.

🔄 Four Phases of Incident Response:

1. **Preparation** – Team readiness and proactive defense
2. **Detection and Analysis** – Identifying and assessing incidents
3. **Containment, Eradication, and Recovery** – Isolate, clean, and restore systems
4. **Post-Incident Activity** – Document findings and improve future defenses

---

🦠 3. Malware Analysis

Malware is any software created with malicious intent, such as viruses, trojans, and ransomware.

🧬 Types of Malware:

- **Virus** – Code that spreads by attaching to programs
- **Trojan Horse** – A seemingly harmless program that performs malicious actions
- **Ransomware** – Encrypts user data and demands ransom for access

🧪 Malware Analysis Techniques:

- **Static Analysis**
  Inspecting malware code without executing it (requires knowledge of assembly).

- **Dynamic Analysis**
  Running malware in a controlled environment to observe its behavior.

> ✅ Learning both **Offensive** and **Defensive** Security prepares you to protect, detect, and respond to real-world cyber threats.